UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/541,667	03/31/2000	Carl M. Ellison	042390.P8629	3630

7590 11/12/2003

Thinh V Nguyen
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard
7th Floor
Los Angelos, CA 90025

EXAMINER	
TRAN, TONGOC	
ART UNIT	PAPER NUMBER
2134	11

DATE MAILED: 11/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PR4

Office Action Summary	**Application No.** 09/541,667	**Applicant(s)** ELLISON ET AL.	
	Examiner Tongoc Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *31 March 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6-10* .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1. This office action is in response to applicants' application serial no. 09/541667 filed on 3/31/2000.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 3/21/02, 7/9/02, 6/3/02, 11/22/02 and 5/6/03 is being considered by the examiner.

Specification

3. The disclosure is objected to because of the following informalities:

Brief Summary of the Invention is missing.

> Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 17-20, 37-40, 57-60, 77-80 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. In respect to claim 17, 37, 57 and 77, the phrase "chipset isolated nub loader hash" and the chipset isolated hash log" are not clearly defined in the specification. Claims 17-20, 37-40, 58-60, 78-80 are rejected because they depend from the rejected claims above.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, 21-25, 41-45 and 61-65 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis (U.S. Patent No. 6,357,004).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

9. In respect to claim 61, Davis discloses a system comprising:

"at least one processor operating in a secure environment, the at least one processor having one of a normal execution mode and an isolated execution mode (see Fig. 2, items 135 and 105, col. 3, lines 55-63);

a memory coupled to the at least one processor, the memory having an isolated memory area accessible to the at least one processor in the isolated execution mode (see col. 3A, item 205 and 210, col. 4, lines 29-41); and

a chipset couple to the at least one processor and the memory, the chipset having a circuit (see Fig. 2, col. 3, lines 55-63), the circuit comprising:

an interface to map a device via a bus to an address space of the chipset in the secure environment (see Fig. 2 and Fig. 3A, col. 3, lines 55-63 and col. 4, lines 58-41), and

a communication storage corresponding to the address space to allow the device to exchange security information with the at least one processor in the isolated execution mode in a remote attestation" (see Fig. 2 and 3A, col. 3, lines 15-30 and 4, lines 48-58).

10. In respect to claim 62, Davis further discloses, "wherein the security information includes at least one of a static public key and a static key certificate" (see col. 3, lines 15-30).

11. In respect to claim 63, Davis further discloses, "wherein the interface comprises: a decoder to decode the address space onto the bus so that an access to the chipset is passed to the device (see col. 4, lines 37-47, decompression).

12. In respect to claim 64, Davis further discloses, "wherein the device accesses a chipset storage via the address space" (see Fig. 2 and col. 3, line 55-col. 4, line 2).
In respect to claim 65, Davis further discloses, "wherein the communication storage comprises: a configuration storage to store device configuration information (see col. 7, lines 5-12).

13. Claims 1-5 are apparatus claims that are substantially equivalent to the system claims 61-67 and therefore are rejected by a similar rationale.

14. Claims 21-25 are method claims that are substantially equivalent to the system claims 61-67 and therefore are rejected by a similar rationale.

15. Claims 41-45 are computer readable medium claims that are substantially equivalent to the system claims 61-67 and therefore are rejected by a similar rationale.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 6-7, 9-17, 26-27, 29-37, 46-47, 49-57, 66-67 and 69-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (U.S. Patent No. 6,357,004) in view of Ermolovich (U.S. Patent No. 4,319,233).

In respect to claim 66, Davis discloses the communication storage as applied to claim 65 but does not explicitly discloses said storage comprises:

"a status register to store device status of the device;

a command register to store a device command for a command interface set; and

an input/output block(IOB) to store input and output data corresponding to the command".

However, Ermolovich discloses a status register to store device status (see col. 85, lines 37-45), a command register to store a device command (see col. 12, lines 2-6) and an input/output block to store input and output data (see col. 71, lines 40-64). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Davis' system of ensuring integrity throughout post processing with the teaching of Ermolovich's communication device with data processing system by including the status register, the command register and the input/output block taught by Ermolovich to prevent data from being lost or corrupted during data transfers between a data processing system and an external device (see Ermolovich et al. abstract and col. 3, lines 26-50)

18. In respect to claim 67, Davis and Ermolovich disclose the system of claim 66. Davis further discloses, "wherein the configuration storage comprises:

a public key storage to store the static public key; a key certificate storage to store the static key certificate (see col. 4, lines 48-58); and

an interface set storage to store an interface set identifier, the interface set identifier identifying a command interface set supported by the device (see col. 4, lines 4, lines 48-58).

19. In respect to claim 69, Davis and Ermolovich disclose the system of 67. Ermolovich further discloses, "wherein the command interface set is an initialization set, the initialization set supporting a reset command and a connect command" (see col. 54, lines 20-28).

20. In respect to claim 70, Davis and Ermolovich disclose a system of claim 67. Davis further discloses "wherein the command interface set is an attestation set, the attestation set performing at least one of a public key enumeration, a key certificate enumeration, and signing operation" (see col. 4, lines 48-53).

21. In respect to claim 71, Davis and Ermolovich disclose the system of claim 70. Ermolovich further disclose, "wherein the status register comprises:

a connection field to provide a connection status to indicate that the device is responsible to the connect command (see col. 9, lines 7-17); and

an estimate field to provide an estimate of processing time for an operation specified in the command" (see col. 16, lines 1-14).

22. In respect to claim 72, Davis and Ermolovich disclose the system of claim 71. Ermolovich further discloses "wherein the status register further comprises:

a self-test field to indicate status of a self test in response to the reset command" (see col. 86, lines 4-21).

23. In respect to claim 73, Davis and Ermolovich disclose the system of claim 70. Davis further discloses, "wherein the public key enumeration enumerates an additional public key than the static public key" (see col. 4, lines 29-36 and lines 48-53).

24. In respect to claim 74, Davis and Ermolovich disclose the system of claim 70. Davis further discloses, "wherein the key certificate enumeration enumerates an additional key certificate other than the static key certificate" (see col. 4, lines 29-36 and lines 48-53).

25. In respect to claim 75, Davis and Ermolovich disclose the system of claim 70. Davis further discloses, "wherein the sign operation generates a signature to attest validity of the secure environment using a private key provided by the chipset" (see col. 2, lines 55-65).

26. In respect to claim 76, Davis and Ermolovich disclose the system of claim 75. Davis further discloses, "wherein the signature corresponds to signing a chipset parameter" (see col. 2, lines 55-65).

27. In respect to claim 77, Davis and Ermolovich disclose the system of clam 76. Davis further discloses, "wherein the chipset parameter is a software hash" (see col. 2, lines 41-54).

28. Claims 6-7 and 9-17 are apparatus claims that are substantially equivalent to the system claims 66-67 and 69-77 and therefore are rejected by a similar rationale.

29. Claims 26-27 and 29-37 are method claims that are substantially equivalent to the system claims 66-67 and 69-77 and therefore are rejected by a similar rationale.

30. Claims 46-47 and 49-57 are computer readable medium claims that are substantially equivalent to the system claims 66-67 and 69-77 and therefore are rejected by a similar rationale.

31. Claim 8, 28, 48 and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (U.S. Patent No. 6,357,004, hereinafter Davis ['004]) and Ermolovich (U.S. Patent No. 4,319,323) as applied to claim 67 above, and further in view of Davis (U.S. Patent No. 5,844,986 hereinafter Davis ['986]).

32. In respect to claim 68, Davis ['004] and Ermolovich disclose the configuration storage as applied to claim 67. Davis ['004] and Ermolovich do not explicitly disclose, "wherein the configuration storage further comprises:

A manufacturer identifier storage to store a manufacturer identifier; and

A revision storage to store a revision identifier. However, Davis ['986] discloses manufacture identifier storage (see col. 3, lines 37-45, software manufacture (BIO vendor), BIO code) and a revision storage to store revision identifier (see col. 4, lines 7-13, revision date). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Davis ['004] and Ermolovich's teachings with Davis' ['986] teaching of storing a manufacturer identifier and revision identifier for the purpose identifying product manufacture and product version information in order to determine product compatibility and perform product upgrade.

33. Claim 8 is an apparatus claim that is substantially equivalent to the system claim 68 and therefore is rejected by a similar rationale.

34. Claim 28 is a mehod claim that is substantially equivalent to the system claim 68 and therefore is rejected by a similar rationale.

35. Claim 48 is a computer readable medium claim and is substantially equivalent to the system claim 68 and therefore is rejected by a similar rationale.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Davis ['816] discloses an optimized security functionality in an electronic system.

-Davis ['147] discloses a system and method for configurating and registering a cryptographic device.

-Davis ['537] discloses a platform and method for assuring integrity of trusted agent communication.

-Davis ['981] discloses an electronic system and method for controlling access through user authentication.

-Davis ['650] discloses a secure public digital watermark.

-Ellison et al. Discloses a controlling access to multiple memory zones in an isolated execution environment.

-Poisner discloses a system for detecting over-clocking users a reference signal thereafter preventing over-clocking by reducing clock rate.

-Drews discloses a system and method for verifying the integrity and authorization of software before execution in a local platform.

-Adams et al. discloses a kernels, description tables and device drivers.

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-9600.

Examiner Tongoc Tran
Art Unit: 2134

TT
October 28, 2003

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134